An Interleaved EPE-Immune PA-DPL Structure for Resisting Concentrated EM Side Channel Attacks on FPGA Implementation

Wei He, Eduardo de la Torre, and Teresa Riesgo

Centro de Electrónica Industrial, Universidad Politécnica de Madrid,

Abstract. Early propagation effect (EPE) is a critical problem in conventional dual-rail logic implementations against Side Channel Attacks (SCAs). Among previous EPE-resistant architectures, PA-DPL logic offers EPE-free capability at relatively low cost. However, its separate dual core structure is a weakness when facing concentrated EM attacks where a tiny EM probe can be precisely positioned closer to one of the two cores. In this paper, we present an PA-DPL dual-core interleaved structure to strengthen resistance against sophisticated EM attacks on Xilinx FPGA implementations. The main merit of the proposed structure is that every two routing in each signal pair are kept identical even the dual cores are interleaved together. By minimizing the distance between the complementary routings and instances of both cores, even the concentrated EM measurement cannot easily distinguish the minor EM field unbalance. In PA-DPL, EPE is avoided by compressing the evaluation phase to a small portion of the clock period, therefore, the speed is inevitably limited. Regarding this, we made an improvement to extend the duty cycle of evaluation phase to more than 40 percent, yielding a larger maximum working frequency. The detailed design flow is also presented. We validate the security improvement against EM attack by implementing a simplified AES co-processor in Virtex-5 FPGA.

Keywords: Interleaved Placement, Dual-Core, Concentrated EM Attack, Routing Conflict, PA-DPL, PIP, LUT, FPGA.

1 Introduction

Power consumption and ElectroMagnetic (EM) attacks are the most studied attack types since Side Channel Attack (SCA) was introduced by Paul Kocher et al [1]. DPL (Dual-rail Pre-charge Logic) is experimentally proved to be an effective countermeasure against SCA by masking its data-dependent power or EM variations due to the complementary behavior between the True (T) and False (F) rails.

In [2], the Early Propagation Effect (EPE), also called Early Evaluation/Pre-charge Effect is first time studied, revealing a potential defect in conventional DPL logic that can possibly impact the complementary balance between T and F rails. The difference

of arrival time for the inputs of complementary gates (or LUTs on FPGA) is potential of generating unintentional data-dependent power or EM peaks. This is particularly critical in FPGA implementation due to the rigid routing resource. In recent years, several countermeasures for repairing the EPE problem were proposed, mainly depending on the use of dual-rail compound gates with complementary signal pairs. In this structure, the corresponding gates from dual rails are set side by side but routings are done automatically by the router, which may lead to non-identical routing paths between the complementary rails. A dual-core structure called PA-DPL (Precharge-Absorbed Dual-rail Precharge Logic) is proposed in [3], which aims to resist EPE problem while keeping routing identical for the implementation on Xilinx FPGA with 6-input LUTs. However, separate placement for dual cores makes it vulnerable to concentrated EM attacks.

In this paper, we present a row-crossed interleaved structure to minimize dual rail unbalances caused by the non-identical routings. The main merit is that the identical routing for complementary net pairs can be maintained between both interleaved dual-cores thereby increasing the resistance to concentrated EM attacks. We also mitigate the rigid timing in [3] by extending signal's duty cycle, which helps to increase the maximum working frequency. The complete design flow and security tests against attacks to interleaved PA-DPL will be given.

The rest of the paper is organized as follows. Section 2 presents an introduction to the EPE problem and briefly discusses related techniques. Section 3 details the proposed interleaved PA-DPL structure with identical routing. Implementation flows of this structure to a simplified AES co-processor are shown in section 4. Section 5 describes the experimental attacks and net delay results. The work conclusion and future work are given in section 6.

2 Related Work

Side channel analysis reveals the confidential information by analyzing side channel leakages from low level, namely physical level. Therefore, countermeasures on this level typically have better security performance than, for example, arithmetic protections. However, physical leakages can be affected by a lot of factors. Any minor asymmetry between the T and F rails can possibly lead to a detectable unbalanced compensation in DPL structure, such as compensation skew, switching time swing or glitch. Typically, routing length and process variation are considered to be two significant factors which impact the compensation between T and F rails [4].

2.1 The Problem of Early Propagation Effect

DPL is a common logic type with symmetrical structure and mirror behavior. DPL generates complementary logic behaviors from T and F rails and therefore obtains constant and stable switching pattern in overall view of power or EM curves from both rails. Figure 1 shows a compound XOR gate where complementary inputs between the 2 gates generate complementary outputs.

Conventional DPL structures may be vulnerable due to EPE. When gates switch either from pre-charge to evaluation phase or from evaluation to pre-charge phase, EPE potentially occurs in these switching actions. Actually, the EPE problem does not just open the possibility of attacks against power/EM variations caused by switching-related glitches or skewed match, but also the switching actions themselves by measuring the time variation. Generally, EPE has 3 main impacts that can be potentially used to launch side channel analysis.

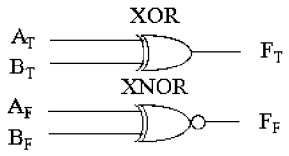

Fig. 1. DPL compound XOR gate, inverter factor is allowed in this example

Unintentional Switch. Normally, DPL logic requires that each compound gate should have and should only have one switch action in each clock cycle to ensure that it's data-independent [18][19]. For the inputs of a gate with variant arrival times, unintentional switch may happen depending on the input combination. As shown in Figure 2, the XOR gate of compound gate XOR has different arrival time, when the combination of inputs are A_T:B_T=1:1 in evaluation phase, a short switching action occurs. It would be inevitably reflected in power or EM leakages. Since only in this input combination the switch can occur. So it can be said that this peak in power or EM trace is data-dependent.

Switching Time. EPE also covers problem in terms of gate switching time. Switching time attack was first introduced in [5]. In DPL, the switching edge for a gate with different input arrival time swings depending on the input combination. In Figure 3, early switching and late switching reveal the input combination as "1:0" and "0:1" respectively. Therefore, starting edge of switching action for this gate is also data-dependent.

Skewed Compensation. The two gates in each compound gate should switch simultaneously so as to match each other precisely. Even if the arrival time for the inputs of each gate of the compound gate can be maintained identical, XOR and XNOR gate cannot switch at the same time because the arrival time between the two gates are not the same (XOR gate 1 unit, XNOR gate 2 units, as shown in Figure 4). The minor peak residue due to skew compensation is still suspicious of attacks.

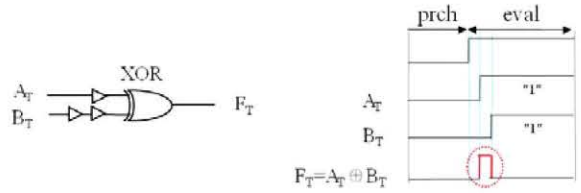

Fig. 2. For this single XOR gate in the XOR compound gate, different input delay leads to data-dependent unintentionally switch action

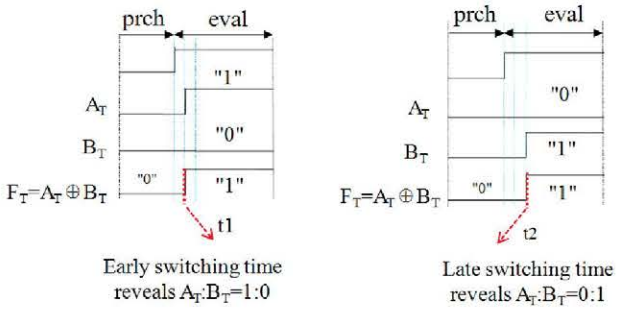

Fig. 3. Switching time swings depending on the input combination of each single gate of the XOR compound gate

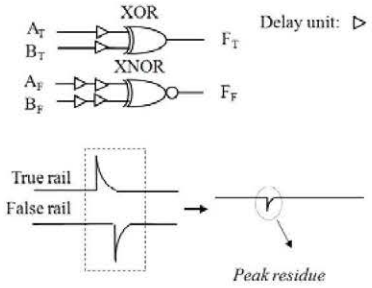

Fig. 4. Skewed switching action causes imperfect match

2.2 Previous Work Related with EPE Protection

For the FPGA implementation, some techniques have been proposed for resisting EPE in recent years. DRSL is introduced in [6], which synchronizes the inputs before the evaluation phase. STTL [20] ensures the same arrival time of the gate inputs by using an extra validation rail. It requires customized unique gate, thereby bringing troubles to the implementation. iMDPL [7], which is developed from MDPL [8], can synchronize the gate inputs with SR-Latch, but the size and complexity of the gate are

concerns. BCDL is presented in [9], which synchronizes all the input pairs of a compound gate by using a Bundle block. Since it has no limitation of gate type, better optimization reduces the resource costs compared with previous ones. Another structure named DPL-noEE [10] evolved from BCDL embeds the synchronization logic into the encoding of LUT equations. Any potential intermediate transition is eliminated by changing the code values to the value of pre-charged invalid state. It has the highest efficiency in resource usage, however the starting edge of the evaluation phase swings depending on the input combination. In [13], authors explored place and route techniques for SDDL logic. which keeps identical routing for both rails in interleaved placement, while EPE problem is not solved yet.

2.3 Interleaved Placement

In FPGAs, logic cells and routing resources are deployed as a highly regular array. Interleaved placement aims to overlap the T and F parts of the dual-rail modules by mapping the synthesized design into the basic logic blocks (the CLBs) side by side. This helps to make the distance of the complementary cells as small as possible. In Xilinx FPGAs, placement configuration is controllable by setting prohibit constraints. Different placement types can be used for an interleaved dual core module. Similar to the work in [13], we investigated several placement types, as shown in Figure 5, due to the merits that type A and B give the smallest distance between complementary instances and nets with high placement density. Comparatively, type C offers a larger space for routing, whereas with lower placement density.

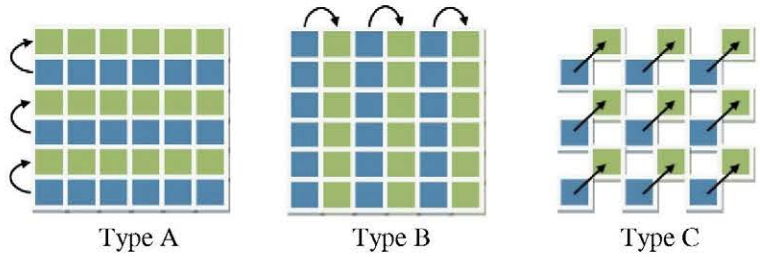

Fig. 5. Possible placement configurations for dual-core interleaved structure

3 Proposal of Interleaved PA-DPL

Due to the fact that pre-charge and synchronization logic are embedded into the LUT equations, PA-DPL has high efficiency in hardware resource usage compared with most of other EPE-resistant solutions. Up to 4 input equations are permitted in 6-input LUT without inverter prohibition, this can further optimize resource usage.

3.1 PA-DPL

PA-DPL evolves from FPGA implemented SDDL logic [11][12]. As mentioned in [3], Pre-charge action logic is absorbed into the LUT function by inserting a global pre-charge signal. Ex signal works together with Pre-charge signal to restrict the evaluation and pre-charge phases into a fixed portion. Pre-charge and Ex are produced with a stable phase shift. The resistance against EPE benefits by the following 2 points [3]:

1. **Early Pre-Charge Prevention.** In PA-DPL, Ex and Pre-charge signals are implemented by global clock networks and directly connected to every LUT in the protected part. So all the logic cells can be pre-charged instantly and simultaneously without waiting for the propagation of the pre-charge waveform as needed in WDDL [11]. Therefore, we can ensure that the pre-charge phase always starts before the invalid data (pre-charged value) of the fastest input arrives at each LUT, as illustrated in Figure 6.

2. **Early Evaluation Prevention.** Since valid data needs to propagate from source registers to capture registers, the Ex signal in PA-DPL acts to confine the evaluation phase into a restricted period in each clock cycle in order to make the evaluation phase to start after the valid data of the slowest input arrives at each LUT. Register stores the propagated valid data in each evaluation phase and then releases it to the first LUT of the next sequential stages in the next evaluation phase. So T and F registers always store complementary valid data.

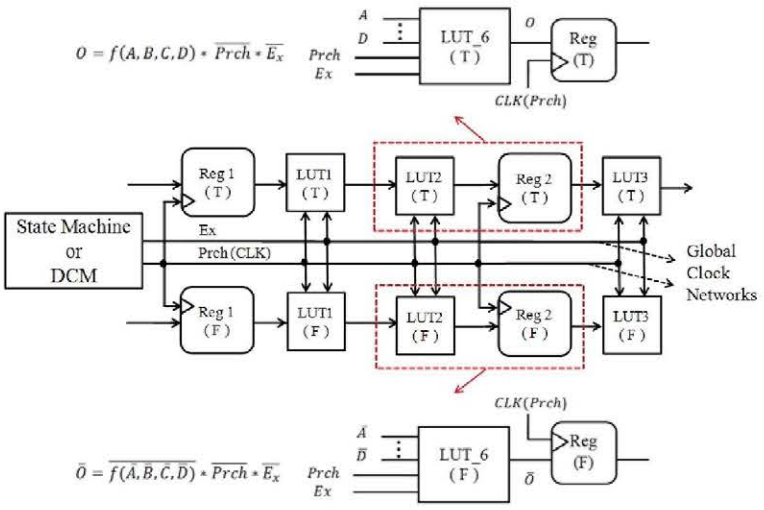

Fig. 6. Implementation of PA-DPL logic [3]

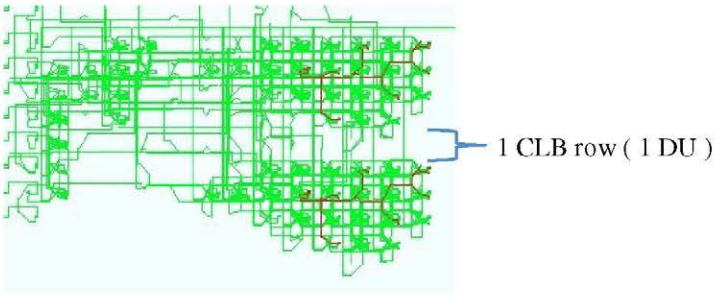

Fig. 7. Separate dual-core structure of PA-DPL logic

Threats from Concentrated EM Analysis. The two cores in PA-DPL can be set close to obtain optimal timing and security performances, as shown in Figure 7, the two cores are placed at a distance of 1 CLB row, hereafter will be called 1 DU (Distance Unit). However, the complementary LUTs and routing are still deployed in locations with relatively larger distances, here 5 DU. If a narrow probe can be set precisely to either one of the two cores, the induced voltage by the magnetic field from a pair of data-dependent cells cannot be balanced.

Power-based attacks depend on the global power consumption of the whole design. So, in this context, location of the core does not have crucial influence in the compensation of the whole power consumption. So, separate architecture for dual core is not a big weakness against power-based side channel analysis. However, manufacturing process variation matters when facing more sophisticated power or EM attacks. In [22][23] authors demonstrated that closer locations in a chip have less process variations. In order to mitigate the fabrication process deviation, it is better to deploy two complementary cells or nets in closer locations.

3.2 Routing Conflicts

Compared with ASIC implementation, FPGAs have much less freedom to choose the resource to be used in the design, specially for the routing resources. Using the FPGA Place and Route tools (PAR), users cannot control the router but following the pre-defined routing algorithm.

Switch matrices offer the connecting possibilities between the horizontal and vertical local lines. Combined with some special interconnects, the router tool automatically connects all logic cells according to the specific design. Generally, Switch Box in perimeters vary with those inside the fabric in the number of allowable routes. Since identical routings require identity in routing resources, the placement for the duplicate part should preferably avoid the use of the perimeter resources so as to prevent the routing problems in advance.

In an interleaved placement, routing conflicts can occur when duplicating the routings of the T core to the location of the F core since the routing resource for the

F core may possibly have been pre-assigned by the nets of the T core. This makes the techniques of direct copy-and-paste in [14] challenging if the F part is overlapped or interleaved in the same fabric location with the T part.

3.3 Timing Improvement

Compared with WDDL, the synchronized logic in [3] has a decreased duty cycle of 25%. Actually, there are timing margin can be obtained. Here, we avoid the use of a frequency-doubled Ex signal, but using one which has the same frequency with the global pre-charge and clock signal, as shown in Figure 8. As well, we use a stable phase shift between Prch and Ex to compress the evaluation phase for making the evaluation phase start only after the valid data (evaluated value) of the slowest input arriving at the gate (i.e. LUT in FPGA). It can be easily done by setting the width of a Johnson Counter to 6 bit (other width can also be chosen depending on the phase shift a specific design requires), and choosing the outputs of any two neighboring bits as the inputs of global clock buffers of Prch and Ex respectively. So, Prch gets 30° phase shift forward to Ex. With this configuration, we can get the synchronized signal with a fixed evaluation phase of 41.7%. This configuration is related with the speed of the circuit. Less phase shift offers larger duty cycle, however it risks of exceeding the arrival time of the slowest input in certain LUT. If the gate mapped to this LUT is critical (i.e. is related to the key of the crypto-algorithm), side channel analysis to this part is still possible. Larger phase shift leads to smaller evaluation phase (i.e. smaller signal duty cycle), however, it prevents EPE in the majority of the critical cells.

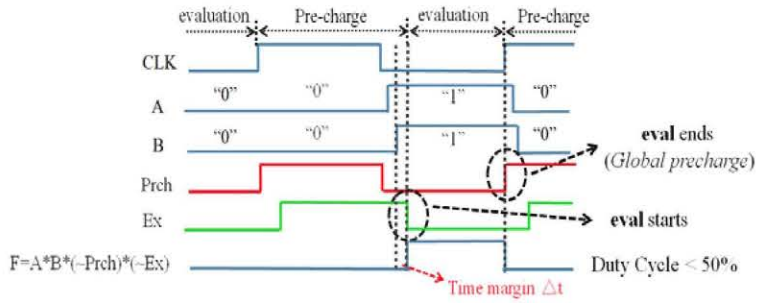

Fig. 8. Timing schedule for interleaved PA-DPL XOR gate

4 Implementation

A simplified AES co-processor is chosen as the testing design for our row interleaved PA-DPL. We implement the SBOX by logic elements instead of RAM. Figure 9 illustrates the block diagram of this design. It contains only XOR operation and SBOX substitution blocks. T and F cores share the same control and clock generation blocks in order to save resources. The partition method used is similar to the technique in [15]. In each clock cycle, 8 bits plaintext generated from a

Pseudo-Random Number Generator (PRNG) is encrypted into 8 bits ciphertext, and it will be abbreviated as AES-8. A pair of 8-bit registers store the outputs from T and F SBOX. Figure 10 shows the design flow of the interleaved PA-DPL. The complete procedure is made up of manual, automatic and routing conflict check phases.

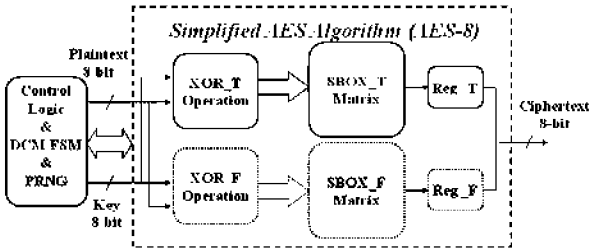

Fig. 9. Block diagram of dual cores simplified AES module

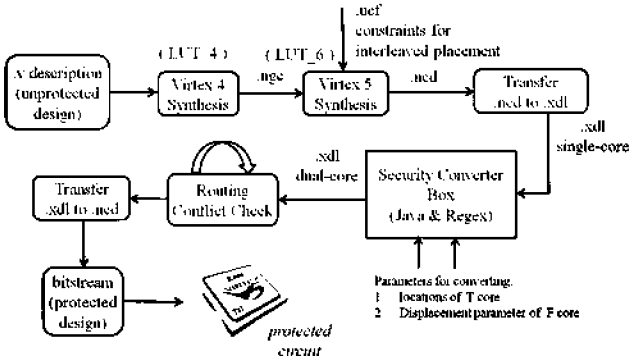

Fig. 10. Dual cores share the same control and clock-generating logics

Manual Phase. This step includes two synthesis iterations, one constraints insertion and one file conversion. First, Virtex-4 is chosen as the target device to synthesize the HDL file of our design. We can get a ngc file which is a binary expressed netlist file with constraint information. The size of each Boolean function in this file is constrained to a 4 input LUT since Virtex-4 FPGAs are based on 4 input LUTs. Then, Virtex-5 is used as the target device to synthesize the ngc file. We set the maximum input number of the 6 input LUT to 4 and disable the optimization strategy in process properties, we then get a ncd file in which all the 6 input LUTs have at most 4 used inputs, namely at least there are 2 unused inputs for each 6 input LUT. This is exactly what is required, because in PA-DPL, 2 inputs of each LUT should be used in order to implement pre-charge and synchronization logics. An ucf file is utilized in this synthesis to limit the use of CLBs in certain parts to make it as a initially interleaved placement. As shown in Figure 11, after the synthesis, the ncd file is then converted to XDL (Xilinx Design Language) version.

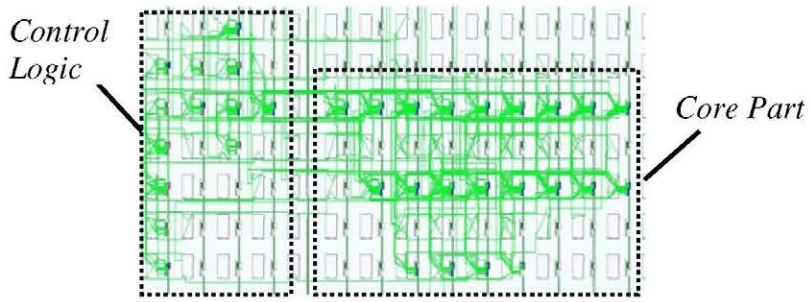

Fig. 11. Single (unprotected) core with row-crossed interleaved placement

Automatic Phase. A XDL file is a readable version of a ncd file. It contains all information of the design with regular format for all instances and nets. Thereby all the copy and paste work can be done by modifying the XDL content using programming languages. Here, we constructed a script, named SCB (Security Converter Box), to automatically and safely convert the single core to an interleaved dual-core module in low level description. SCB is compiled with Java and Regular Expression syntax. It can be self-adapted to different designs since users just need to supply two parameters, location of T part (the part needs to be protected) and displacement parameter for the F part (for the Type C placement from Figure 5, this parameter is vertical '+1', horizontal '0'). SCB automatically executes all the modifications and produces a converted XDL file. This phase performs the following steps:

- *Tag nets and instances according to the location parameters*
- *Duplicate and move instances of T part to location of F part.*
- *Insert Prch and Ex to free inputs of LUT*
- *Adjust LUT equation*
- *Arrange over-block nets (delete and convert the nets)*

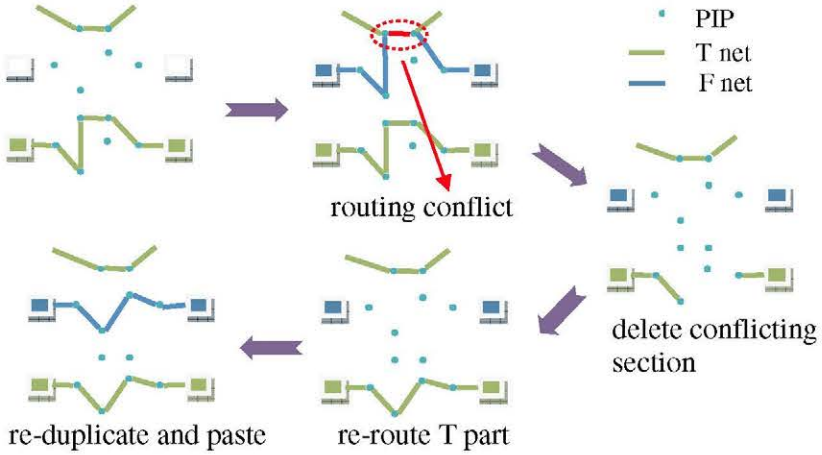

Fig. 12. T net is routed by Xilinx router, so it has optimal global timing result. In this check and re-route flow, it deletes the conflict net section and maintain all the other sections. So, the optimized timing result provided by router can be maintained as much as possible.

Routing Conflict Check Phase. After the conversion step, a PA-DPL protected circuit in interleaved structure is obtained. Then it is transformed back to ncd file. At this point, conflicts between the T and F routing lines may potentially exist in the design. So, the design is checked by a tool developed on top of RapidSmith [16][17]. This tool transforms every net to an abstract representation where every net is represented as a node, and Programmable Interconnect Points (PIPs) define the connections between these nodes. Since we've tagged the copied routing lines in the previous phase, the tool checks all routing information of the F part by comparing the path shape (PIPs information) between T and F rails. If two same PIPs are found, the F routing passing through this PIP conflicts with another routing which passes through the same PIP. It then deletes the conflict section of the T routing, re-route it and duplicates it to generate a new F routing. Then, the tool checks PIPs of the new F routing again. If there are conflicts again, the procedure is repeated until no conflicts are found. Figure 12 illustrates the block diagram of this check and re-route flow.

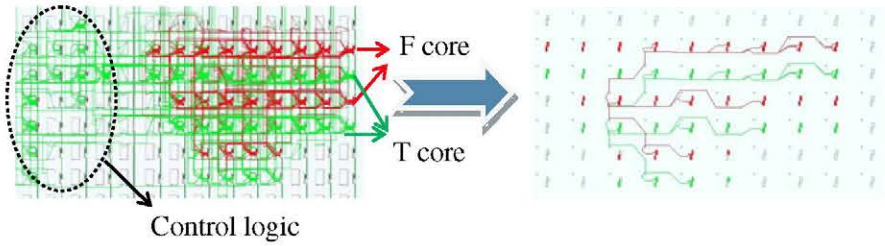

Fig. 13. Dual-core (protected) with row-crossed interleaved placement. Complementary routing pairs in the core part are identical in shape.

The final layout of a PA-DPL AES-8 in row-crossed interleaved structure is shown in the left part of Figure 13. It has identical routings between the two core parts. By making different placement constraints in manual phase, different interleaved structures can be obtained. However, according to the test results, we found that the configuration of the PIPs in the horizontal direction are not strictly identical in neighboring columns from the target device (Xilinx Virtex-5). So we eventually choose the row-crossed type (i.e. Type A in Figure 5), due to its high placement density and perfect regularity of PIP configuration in vertical direction. A pair of the identical routing from interleaved placement is shown in the right part of Figure 13.

5 Test Attacks and Timing Check

Comparison attacks are made to validate the protection improvements. We implement AES-8 co-processor in SE (Single Ended, i.e. unprotected), separated PA-DPL and row-crossed interleaved PA-DPL respectively. They are all deployed in the similar fabric location in a same Virtex-5 FPGA chip in order to minimize the interference from process variation [21][22]. Control logic sends the plaintext and repeatedly runs the encryption core at a frequency of 3MHz. SE and separate PA-DPL design also use

the same placement constraints as the interleaved one for the convenience of the comparison. A self-made EM probe (copper multi-turn antenna with 0.5mm diameter and 26 turns) is used to gather EM radiation. Sampling rate is 667MSa/s using an Agilent Oscilloscope with segmented memory.

5.1 Experimental Attacks

Primitive analysis results show that only 60 traces are enough to retrieve the right key in attack to SE implemented AES-8. Separate dual-core PA-DPL resists the attack until the analyzed trace number reaches around 50,000. For the interleaved one, the key revealed trace number is increased to 62,000, gaining increase robustness factors of 1033 and 1.24 respectively from SE one and separate dual-core PA-DPL. Test results are plotted in Figure 14.

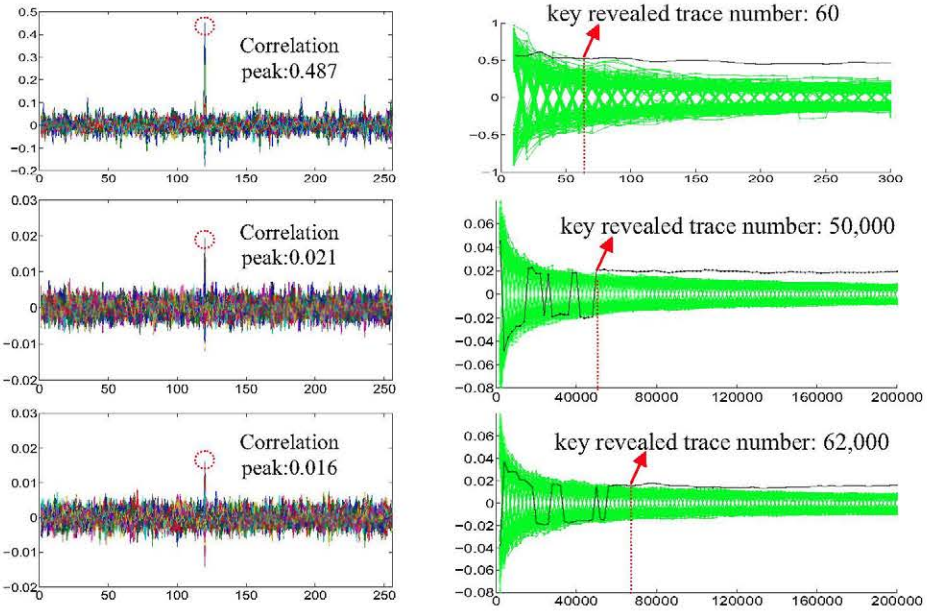

Fig. 14. Correlation Coefficient curves of concentrated EM attacks. The one with interleaved placement shows improved protection level compared with the one with separate placement.

5.2 Timing Verification

FPGA Editor offers a user-oriented interface for convenience of identifying the cells in the fabric matrix, but it doesn't strictly follow the facts on the physical level of the chip. Low level (i.e. physical level) parameters are typically kept confidential from users. Therefore, we made timing comparison between the T and F routings to verity the improvement. Table 1 and Figure 15 show the comparison result. Group II is the

net delay comparison of the complementary nets from an interleaved placement, route uncontrolled dual-core AES-8. Group I is the result of the same module with Group II except using the identical routing methods. It's obvious that in Group I, for most of the nets, difference of net delay is 0 ns. Only few of them have minor difference, less than 20ps. Comparatively, in Group II, since nets are automatically routed by routers, most all of the complementary routing pairs have distinct time delay. The minor delay differences in Group I are caused by the tiny net adjustment when the router connects the new core (F core) and the peripheral control logic. Test result validates the assumption that even if the physical level is unknown, identical nets in FPGA Editor view obtains the same net time delays.

Table 1. Delay difference comparison between Group I (interleaved placement with identical routing) and Group II (interleaved placement without identical routing) of a routing pair with 11 net sections

		net1	net2	net3	net4	net5	net6	net7	net8	net9	net10	net11
I	*net_F*	0.423ns	0.728ns	0.496ns	1.060ns	0.446ns	0.980ns	0.548ns	1.125ns	0.758ns	0.164ns	0.626ns
	net_T	0.423ns	0.728ns	0.496ns	1.060ns	0.446ns	0.982ns	0.548ns	1.143ns	0.758ns	0.164ns	0.626ns
	net_F-net_T	0.000	0.000	0.000	0.000	0.000	-0.002	0.000	-0.018	0.000	0.000	0.000
II	*net_F*	0.421ns	0.686ns	0.494ns	1.058ns	0.443ns	1.125ns	0.529ns	1.124ns	0.759ns	0.410ns	0.626ns
	net_T	0.423ns	0.728ns	0.496ns	1.060ns	0.446ns	0.982ns	0.548ns	1.143ns	0.758ns	0.164ns	0.626ns
	net_F-net_T	-0.002	-0.042	0.002	-0.002	-0.003	0.143	-0.019	-0.019	0.001	0.246	0.000

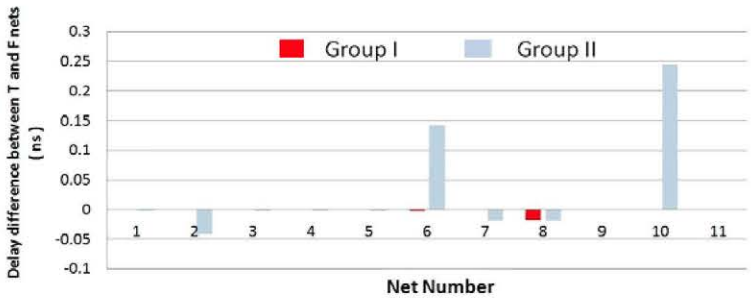

Fig. 15. Bar diagram of time delay difference. Comparison proves that with identical routings, complementary net pairs have extremely small swing of delay time difference.

6 Conclusion

This paper deals with the routing problem which occurs when overlapping the complementary parts of dual-core structures in DPL logic. In our proposal, we developed a technique which is capable of checking and repair the unmatched routing pairs. By following the routing conflict checking flow, identical routing can be kept for the complementary parts, even if the placement is closely interleaved together. Based upon an EPE-resistant PA-DPL, we demonstrated an improved one which has a

row-crossed interleaved structure for the core part with routing consistency. This makes the corresponding complementary instances and nets as close as one DU while the time delays for complementary nets are kept identical. This effectively strengthens the resistance against concentrated EM attacks. Meanwhile, interleaved PA-DPL makes the dual rails closely paralleled. This helps to reduces the process variation impact since neighboring areas in silicon chip provably have more similar electric parasitic parameters than that between two areas apart [22]. We also corrected the Ex signal in PA-DPL to release the timing pressure caused by the compressed evaluation phase. After this improvement, signal duty cycle can be expanded to 41.7% when the core works in 3MHz working frequency. Timing verification validates that the combination of the proposed techniques significantly reduced the time delay differences in each complementary net pairs. Size comparison is made by comparing LUT cost. Interleaved PA-DPL AES-8 occupies 353 LUTs, with an increase factor of 2.69 compared with 131 LUT cost of the unprotected one. Separate PA-DPL one occupies 355 LUTs. This minor difference between interleaved and separate ones is due to the different placements used which impacts the synthesis and mapping results. Cost increase factor varies depending on what proportion the core part accounts for in the whole circuit. The comparison attacks on different implementations show that row-crossed interleaved PA-DPL has an increased resistance against concentrated EM analysis by a factor of 1033 and 1.24 respectively from the unprotected circuit and PA-DPL protected circuit with separate placement.

In the next step, we will test the circuit with more sophisticated attacks in order to make thorough security verifications. Reducing the transient peak current is another part of the future work.

Acknowledgments. This work was partially supported by the Artemis program under the project SMART (Secure, Mobile Visual Sensor Networks Architecture) with number ARTEMIS-2008-100032 and RECINTO project partially funded by Community of Madrid.

1. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
2. Suzuki, D., Saeki, M.: Security Evaluation of DPA Countermeasures Using Dual-Rail Precharge Logic Style. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 255–269. Springer, Heidelberg (2006)
3. He, W., De La Torre, E., Riesgo, T.: A Precharge-Absorbed DPL Logic for Reducing Early Propagation Effects on FPGA Implementations. In: 6th IEEE International Conference on ReConFigurable Computing and FPGAs, Cancun (2011)
4. Guilley, S., Chaudhuri, S., Sauvage, L., Graba, T., Danger, J.-L., Hoogvorst, P., Vong, V.-N., Nassar, M.: Place-and-Route Impact on the Security of DPL Designs in FPGAs. In: HOST, pp. 29–35. IEEE Computer Society (2008)
5. Guilley, S., Chaudhuri, S., Sauvage, L., Graba, T., Danger, J.-L., Hoogvorst, P., Vong, V.-N., Nassar, M.: Shall we trust WDDL? In: Future of Trust in Computing, Berlin, vol. 2 (2008)
6. Chen, Z., Zhou, Y.: Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 242–254. Springer, Heidelberg (2006)

7. Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 81–94. Springer, Heidelberg (2007)
8. Popp, T., Mangard, S.: Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 172–186. Springer, Heidelberg (2005)
9. Nassar, M., Bhasin, S., Danger, J.-L., Duc, G., Guilley, S.: BCDL: a High Speed Balanced DPL for FPGA with Global Precharge and No Early Evaluation. In: Proc. Design, Automation and Test in Europe, pp. 849–854. IEEE Computer Society, Dresden (2010)
10. Bhasin, S., Guilley, S., Flament, F., Selmane, N., Danger, J.-L.: Countering Early Evaluation: an Approach towards Robust Dual-Rail Precharge Logic. In: WESS. ACM, Arizona (2010)
11. Tiri, K., Verbauwhede, I.: A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In: Proc. Design, Automation and Test in Europe, pp. 246–251. IEEE Computer Society (2004)
12. Velegalai, R., Kaps, J.-P.: DPA Resistance for Light-Weight Implementations of cryptographic Algorithms on FPGAs. In: IEEE (FPL) Field Programmable Logic and Applications, pp. 385–390 (2009)
13. Velegalati, R., Kaps, J.-P.: Improving Security of SDDL Designs Through Interleaved Placement on Xilinx FPGAs. In: 21st IEEE International Conference on Field Programmable Logic and Applications, Crete, Greece (2011)
14. Yu, P., Schaumont, M.: Secure FPGA circuits using Controlled Placement and Routing. In: 5th IEEE International Conference on Hardware/Software Codesign and System Synthesis, pp. 45–50 (2007)
15. Kaps, J.-P., Velegalati, R.: DPA Resistant AES on FPGA using Partial DDL. In: IEEE FCCM, Symposium on Field-Programmable Custom Computing Machines, pp. 273–280 (2010)
16. Lavin, C., Padilla, M., Lamprecht, J., Lundrigan, P., Nelson, B., Hutchings, B.: RapidSmith: Do-It-Yourself CAD Tools for Xilinx FPGAs. In: 21st IEEE International Conference on Field Programmable Logic and Applications, pp. 349–355 (2011)
17. Lavin, C., Padilla, M., Lamprecht, J., Lundrigan, P., Nelson, B., Hutchings, B.: HMFlow: Accelerating FPGA Compilation with Hard Macros for Rapid Prototyping. In: 18th IEEE Symposium on Field-Programmable Custom Computing Machines, Salt Lake City, USA (2011)
18. Kulikowski, K., Karpovsky, M., Taubin, A.: Power Attacks on Secure Hardware Based on Early Propagation of Data. In: IEEE, IOLTS, pp. 131–138. Computer Society (2006)
19. Suzuki, D., Saeki, M.: An Analysis of Leakage Factors for Dual-Rail Pre-charge Logic style. IEICE, Transactions on Fundamentals of Electronics, Communications and Computer Sciences E91-A(1), 184–192 (2008)
20. Soares, R., Calazans, N., Lomné, V., Maurine, P.: Evaluating the Robustness of Secure Triple Track Logic through Prototyping. In: 21st Symposium on Integrated Circuits and System Design, pp. 193–198. ACM, New York (2008)
21. Stine, B., Boning, D., Chung, J.: Analysis and Decomposition of Spatial Variation in Integrated Circuit Processes and Devices. IEEE Tran. on Semiconductor Manufacturing, 24–41 (1997)
22. Sedcole, P., Cheung, P.: Within-die Delay Variability in 90nm FPGAs and Beyond. In: Proc. IEEE International Conference on Field Programmable Technology (FPT 2006), pp. 97–104 (2006)
23. Maiti, A., Schaumont, P.: Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive. J. Cryptology 24, 375–397 (2010)